NSTISSI No. 4014
August 1997

NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY OFFICERS (ISSO)

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. This instruction establishes the minimum course content or standard for the development and implementation of training for Information Systems Security Officers (ISSO) in the disciplines of telecommunications security and information systems (IS) security. Please check with your agency for applicable implementing documents.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

NATIONAL SECURITY AGENCY
NSTISSC SECRETARIAT
ATTN: V503 STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

KENNETH A. MINIHAN
Lieutenant General, USAF

NATIONAL TRAINING STANDARD
FOR
INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

SECTION

PURPOSE I
APPLICABILITY II
RESPONSIBILITIES III

SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of training for Information Systems Security Officers (ISSO) in the disciplines of telecommunications and information system (IS) security.

SECTION II - SCOPE APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive No. 501 establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible. This instruction is the continuation of a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (NSTISSI Nos. 4011, 4012, 4013, and 4014). The definitions for words used in this instruction are derived from the National INFOSEC Glossary, NSTISSI No. 4009. The references pertinent to this instuction are listed in ANNEX B. Other documents which can be used in conjunction with this document are listed in ANNEX C.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, the General Services Administration (Office of Information Security), and Government contractors, as well as from adaptations of existing department/agency training programs, or from a combination of experience and formal training. ANNEX A lists the minimal INFOSEC performance standard for an ISSO.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the the development and implementation of training for ISSOs in the disciplines of telecommunications and IS security.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that ISSOs (or their equivalents) are made aware of the body of knowledge as outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

a. maintain and provide an INFOSEC training standard for ISSOs to U.S. Government departments and agencies;

b. ensure that appropriate INFOSEC training courses for ISSOs are developed; and

c. assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC training activities for ISSOs as requested.

ANNEX A

INFOSEC PERFORMANCE STANDARD FOR THE ISSO (ENTRY, INTERMEDIATE & ADVANCED LEVELS)

Job functions using competencies identified in:

DoD 5200.28-M, Automated Data Processing Security Manual
NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems
DCID 1-16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks

The INFOSEC functions of an ISSO are:

(1) maintaining a plan for site security improvements and progress towards meeting the accreditation;
(2) ensuring the IS is operated, used, maintained, and disposed of in accordance with security policies and practices;
(3) ensuring the IS is accredited and certified if it processes sensitive information;
(4) ensuring users and system support personnel have the required security clearances, authorization and need-to-know; are indoctrinated; and are familiar with internal security practices before access to the IS is granted;
(5) enforcing security policies and safeguards on all personnel having access to the IS for which the ISSO is responsible;
(6) ensuring audit trails are reviewed periodically (e.g., weekly, daily), and audit records are archived for future reference, if required;
(7) initiating protective or corrective measures;
(8) reporting security incidents in accordance with agency-specific policy, such as DOD 5200.1-R , to the designated approving authority (DAA) when an IS is compromised;
(9) reporting the security status of an IS, as required by the DAA; and
(10) evaluating known vulnerabilities to ascertain if additional safeguards are needed.

Terminal Objective:

ENTRY LEVEL: Given a series of hypothetical system security breaches, the ISSO will identify system vulnerabilities and recommend security solutions required to return the systems to operational level of trust.

INTERMEDIATE LEVEL: Given a proposed new system architecture requirement, the ISSO will investigate and document system security technology, policy and training requirements to assure system operation at a specified level of trust.

ADVANCED LEVEL: Given a proposed IS accreditation action, the ISSO will analyze and evaluate the system security technology, policy, and training requirements in support of DAA approval to operate the system at a specified level of trust. This analysis will include a description of the management/technology team required to successfully complete the accreditation process.

List of performance items under job functions

E = entry level

I = intermediate level
A = advanced level

In each of the competency areas listed below by job function, the ISSO shall perform the following functions at the levels indicated:

1. Maintain a plan for site security improvements and progress towards meeting the accreditation

a. Facilities

(1) Planning

E - cite significance of facilities planning in INFOSEC;
E - identify issues that need to be addressed in facilities plan; make suggestions for enhancement to plan; and
I - review facility plan and make suggestions for upgrades and modifications to enhance INFOSEC posture;

(2) Management

E - list basic principles of facility management; and
I - ensure the plan is implemented as planned.

(3) Housekeeping

E - list general procedures in facility, e.g., standard operating procedures (SOP), access roster, etc.;
I - develop the SOP, maintain the access roster.

(4) Data Processing Center (DPC) Security

E - list unique security requirements above and beyond general facility management for DPCs.

b. INFOSEC Program Planning

E - describe the overall program to users and managers;
E - prepare input to the overall security plan;
I - prepare the plan;
I - present the plan to management and users; and
I - propose changes to the plan.

(1) Procedures

E - describe the policy, etc. to users and managers;
E - identify potential flaws in policy, etc., and initiate corrective actions;
E - provide periodic reports to managers with status and recommendations;
I - write the procedures as required;
I - design the procedures and test them; and
I - modify procedures as required.

(2) Contingency Plans

E - prepare input to contingency plan;
E - write the contingency plan;
E - identify items for which plans must be developed; and
I - modify the contingency plan to reflect changes.

(3) Continuity Plans

E - prepare input to continuity plan;
E - write the continuity plan;
E - identify items for which plans must be developed; and
I - modify the contingency plan reflecting changes.

(4) Emergency Destruction Procedures (EDP)

E - explain the EDP to those who execute the plans;
E - ensure executors of EDP plans are trained in environmental and safety issues;
I - demonstrate the EDP to users and managers; and
I - integrate EDP into overall plans.

(5) Network Monitoring

E - list capabilities, limitations, and data available from network monitors;
E - identify networks to be monitored including times and amount/types of data to be collected;
E - ensure laws, for instance, warning banners in place, are followed;
I - determine the need to monitor suspicious activity; start the monitoring process; and
I - justify to management the need for the detailed monitoring.

(6) Password Management

E - list the underlying password management principles explaining the need for password management;
E - issue passwords to users; ensure that passwords are chosen in accordance with policy; disable accounts when necessary;
E - address questions or concerns of users and managers; and
I - develop local policies and procedures for password management in accordance with higher level policies, etc.

(a) Password Sharing

E - inform users they are not to share passwords and the consequences of doing so (explain the potential criminal penalties involved);
I - identify abuses, e.g., who is sharing passwords or files; and
I - propose methods to share files without sharing passwords.

(b) Password Choosing

E - describe to users how to choose appropriate passwords, and how/why to protect them;
I - enforce good selection of passwords in accordance with password management practices, and also notify user/managers of violations for appropriate action; and

I - provide examples of good and bad passwords as an awareness activity.

(7) Rules-based Access Controls (RBAC)

E - define RBAC;
I - integrate the access controls into the appropriate operating plans, procedures, etc.; and
I - ensure the access controls are properly and correctly installed in accordance with the security policy.

(8) Protection from Malicious Code

E - describe malicious code and outline the various types of malicious code;
E - describe techniques for protection from malicious code to users, and provide examples (real and theoretical);
E - report suspected or actual occurrences of malicious code and initiate corrective actions as appropriate;
I - propose methods and policies to combat introduction of malicious code into a site; and
I - integrate protection techniques into the system and into policies.

c. Administrative Security

E - outline the components of administrative security;
E - prepare input to the administrative security plan for which he/she is responsible;
E - implement parts of plan for which he/she is responsible;
E - report to management on variations from the plan and suggest improvements to the plan;
I - modify the administrative security plan in accordance with higher level policies; and
I - enforce the plan.

2. Ensure the IS is operated, used, maintained, and disposed of in accordance with security policies and practices

a. Laws, Regulations, and Other Public Policy

E - outline INFOSEC policy, laws, and regulations, and explain their relevance to users;
E - ensure all system use is in adherence to the policy, etc.;
E - answer questions from users and interpret the rules;
E - implement adherence, remind users of rules;
E - notify management and users of status and violations of the rules;
I - enforce reporting to management of variances from the laws, regulations, etc.; and
I - develop the local policies and procedures based on rules, regulations, etc.

(1) Information Systems Security Policies

E - identify national policies;
E - prepare input to the policies;
E - tell users of the policies, and interpret the policy;

E - report variations from policy;

I - identify areas where policies need to be prepared;

A - interpret policies for unique situations not specifically covered by policy;

A - influence the priority in which policies are developed, and their implementation;

A - review draft policies and procedures from all levels prior to being finalized; and

A - verify policies and procedures are accomplishing their intended goals and supporting the overall security policy.

(a) COMSEC

E - outline basic COMSEC principles;

E - describe uses of COMSEC to users;

E - ensure appropriate COMSEC measures are used;

I - evaluate COMSEC procedures as they apply to a system;

I - integrate COMSEC procedures into the system;

I - report COMSEC violations in accordance with appropriate policy;

I - help users and managers with the interpretation and implementation of COMSEC policies and techniques;

A - verify COMSEC policies are in place and accomplishing the intended goals, and are supporting the overall security policy; and

A - perform independent audits of implementation of COMSEC procedures with respect to policy.

(b) Computer Security (COMPUSEC)

E - outline basic COMPUSEC principles;

E - describe uses of COMPUSEC to users;

E - ensure appropriate COMPUSEC measures are used;

I - evaluate COMPUSEC procedures as they apply to a system;

I - integrate COMPUSEC procedures into the system;

I - report violations in accordance with appropriate policy;

I - help users and managers to understand and implement COMPUSEC policies and procedures;

A - verify policy is in place, is accomplishing the intended goals, and supporting the overall security policy; and

A - perform independent audits of implementation of COMPUSEC procedures with respect to policy.

(c) TEMPEST

E - outline basic TEMPEST principles (including zoning concept);

E - identify the Certified TEMPEST Technical Authority (CTTA);

E - describe the uses of TEMPEST to users;

E - ensure appropriate TEMPEST measures are used;

I - integrate TEMPEST procedures into the system;

I - report violations in accordance with appropriate policy;

I - help users and managers to understand and implement TEMPEST techniques and policies;

A - verify policy is in place, is accomplishing the intended goals, and is supporting the overall security policy; and

A - perform independent audits of implementation of TEMPEST procedures with respect to policy.

(d) Operations Security (OPSEC)

E - describe the OPSEC process;
E - describe the objectives of applying the OPSEC process;
E - compare the five elements of risk management and OPSEC processes;
E - describe the relationship between INFOSEC and OPSEC;
E - explain why OPSEC is applicable to any time-definable, supported, organizational activity occuring in an adversarial or competitive environment;
E - ensure users understand OPSEC is not a security compliance oriented process, and there are no "violations";
I - describe how the OPSEC process is applied, and how IS vulnerabilities are thereby identified;
I - describe the unlimited, "anything that works" nature of countermeasures in the OPSEC repertoire;
A - describe how IS risk is assessed using the OPSEC process; and
A - compare and contrast need for OPSEC with respect to mission and costs.

(e) Technical Security (TECHSEC)

E - outline TECHSEC principles;
E - describe uses of TECHSEC to users;
E - ensure TECHSEC measures are used;
I - evaluate TECHSEC procedures as they apply to the system;
I - integrate TECHSEC procedures into the system;
I - report violations in accordance with appropriate policy;
I - help users and managers to understand and implement TECHSEC techniques and policies;
A - verify policies are in place, are accomplishing the intended goals, and supporting the overall security policy;
A - perform independent audits of implementation of TECHSEC procedures with respect to policy; and
A - discuss need for TECHSEC with respect to mission and costs.

(2) Privacy (Privacy Act of 1974)

E - outline the Act and explain its implications;
E - describe to users the relevance of the Act;
E - ensure there is compliance with the Act;
E - notify management of abuse, and know this is a legal issue with civil and criminal consequences;
I - evaluate whether procedures are in compliance with the Act;
I - distinguish what is covered by the Privacy Act and what is not with respect to release of information;
A - influence users and managers to comply with the Act; and
A - validate that policy conforms to the Privacy Act.

(3) Rainbow Series

E - describe scope and purpose of the Rainbow Series of documents;
E - identify the portions needed to be implemented in the system;
E - describe the significance of the Series;
I - apply the Series in an actual system;
I - integrate underlying principles into the system and into security policy;
A - justify variances with the Series to the appropriate authority; and
A - interpret extensions to the Series to situations not specifically addressed.

(a) Trusted Computer Systems Evaluation Criteria (Orange Book);
(b) Trusted Network Interpretation (Red Book); and
(c) Federal Criterion, Common Criteria, Canadian Criteria, others.

(4) International Security Considerations (ISC)

E - outline ISC;
E - describe international INFOSEC programs; and
A - interpret international requirements as they apply to local systems.

(5) Monitoring (e.g., keystroke, banner)

E - outline keystroke monitoring and the underlying laws and requirements for keystroke banners;
E - describe monitoring to users and managers, including what it is, why it is used, and associated civil and criminal consequences;
E - comply with all the rules, regulations, and laws for monitoring;
I - integrate the underlying national policies into practices and procedures;
I - modify local policies to meet the specific situation;
A - validate implementing procedures are in line with the rules, and are used only in approved situations; and
A - verify activation of the monitoring is in accordance with policy, and is justified by the situation.

(6) Profiles

E - define security profiles and explain their relationship to the Orange Book; and
E - describe to users and managers what security profiles are and how they are used.

b. Standards of Conduct (SOC)

E - provide guidance to users or notify users where they can obtain further assistance regarding standards of conduct; and
I - identify the standards of government conduct to include in policy and procedures.

(1) Ethics

E - define IS security ethics;
E - demonstrate ethical IS practices;
E - describe basic ethical procedures (e.g., software license, plagiarism of software, violations of copyright);
I - ensure all software has a valid license;
I - notify management of infractions and include extent of the problem; and

I - develop policies and procedures for software license management.

(2) Fraud, Waste, & Abuse (FW&A)

E - describe examples of IS FW&A;
E - report to management where IS FW&A is occurring;
E - list corrective measure for IS FW&A;
E - provide basic guidance, and refer detailed questions to legal authority;
I - propose policies and procedures to counter and mitigate IS FW&A; and
I - develop methods to address problems as they arise.

c. Generally Accepted Systems Security Principles

E - answer questions from users and interpret the rules;
E - monitor adherence to the rules and remind users of rules;
E - notify management and users of status and violations of the rules;
I - identify the standards upon which the generally accepted systems security principles (GASSP) are based;
I - integrate the GASSP into standard operating procedures; and
I - develop the policies and procedures to reflect the standards.

d. Access Control Model (ACM)

E - define ACM and explain its relationship to security;
E - describe to users and managers what ACMs are and how they are used;
I - develop the policies and models;
I - identify controls for specific systems;
I - integrate the ACM's principles into the operational systems;
I - enforce the ACM policies;
A - review the policies in effect for effectiveness; and
A - change the underlying policies and procedures when necessary.

e. Access Authorization

E - outline access authorization policies and procedures, and explain their relevance to users;
E - describe to users and managers the following mechanisms, including what they are and how they are used:

- Mandatory Access Controls (MAC),
- Discretionary Access Controls (DAC), and
- Identification & Authentication (I&A);

I - modify MAC tables as necessary;
I - review adequacy of MAC to adhere to security policy goals;
I - design and implement DAC practices to conform with policy;
A - verify DAC practices meet the security model goals;
I - integrate I&A practices into system operations;
I - select specific systems where I&A is to be used; and
I - modify system I&A, in accordance with policy to accommodate system-unique environment/circumstances.

f. Accountability

E - define who has the responsibility for accountability;
E - describe the accounting process for hardware, software, and information;
E - outline accountability process/program; and
A - validate the assigned responsibilities are commensurate with underlying IS security policies and are appropriately assigned.

(1) Key Management

E - outline national & agency key management policies and procedures, and explain their relevance to users;
E - describe to users and managers what key management is, and how/why it is used;
E - use key management in a system;
I - design specific procedures for the system in line with policies;
I - integrate key management into the overall system and procedures; and
A - resolve conflict with procedures and policies, and variances thereof.

(a) Electronic Key Management System (EKMS)

E - outline EKMS policies and procedures and explain their relevance to users;
E - describe to users and managers what EKMS is, and how/why it is used;
I - use the appropriate EKMS system;
E - demonstrate knowledge of how to operate an EKMS system;
I - prepare the EKMS operating procedures for a system;
I - identify the components of EKMS as it applies to the system on hand; and
A - verify procedures are in line with policy.

(b) Public Key Encryption (PKE)

E - outline PKE national policies and procedures and explain their relevance to users;
E - describe to users and managers what PKE is, and how/why it is used;
I - implement appropriate public key encryption algorithm;
I - describe PKE methodology;
A - evaluate PKE process for a system; and
A - compare differing public PKE methodologies.

(c) Key Escrow

E - list national key escrow policies and procedures; and
E - describe to users and managers what key escrow is, and how/why it is used.

(d) COMSEC Custodian

E - list national COMSEC custodian policies and procedures, and explain their relevance to users/COMSEC custodians;
E - explain to users and managers what the COMSEC custodian process is and how it is relevant to them;

E - identify uses for COMSEC material on the system;
E - use services and advice of COMSEC custodian; and
A - review local COMSEC policies and procedures from an INFOSEC security standpoint.

(2) Electronic Records Management

E - outline the electronic records management program and underlying rules; and

E - use records management program and describe any effect on the system.

(a) Records Retention

E - define the electronic records management program and underlying rules; and
E - list uses of record retention and describe effect on the system.

(b) E-Mail

E - describe the local e-mail system and its potential vulnerabilities.

(1) Retention

E - describe retention policies as they apply to the system.

(2) Non-Repudiation

E - describe non-repudiation and its application to the system.

(3) Hardware Asset Management

E - describe the hardware asset management program and how it applies/is used on the system.

(4) Software Asset Management

E - describe the software asset management program and how it applies/is used on the system with emphasis on license and copyright issues, and cross reference to ethics;
I - enforce policies and procedures;
I - report non-compliance;
I - promote compliance; and
A - develop policies and procedures.

3. Ensure the IS is accredited and certified if it processes sensitive information

a. Certification Function

(1) Assessments (e.g., surveys, inspections)

E - develop assessments for the purpose of certifying an IS;
E - prepare assessments for use during the certification of an IS; and

I - review assessments for the purpose of certification of an IS.

(2) Verification and Validation Process

A - direct the verification and validation process as part of the certification of an IS.

(3) Technical Certification

A - direct the technical certification of an IS.

b. Accreditation Function

(1) Users

E - direct the efforts of users in the accreditation process.

(2) System Administrator (SA)

E - direct the efforts of the SA in the accreditation process.

(3) Managers

E - direct the efforts of Managers in the accreditation process.

(4) ISSO

E - initiate the accreditation process;
I - organize the accreditation process;
A - complete the accreditation process; and
A - obtain DAA approval.

4. Ensure users and system support personnel have the required security clearances, authorization, and need-to-know, are indoctrinated, and are familiar with internal security practices before access to the IS is granted

a. Personnel

(1) Position Sensitivity

E - identify sensitive positions; and
I - justify sensitive positions.

(2) Disgruntled Employees

E - identify characteristics of disgruntled employees; and
I - monitor access of identified disgruntled employees.

(3) Separation of Duties

A - direct the separation of duties of personnel in accordance with established policies and procedures.

(4) Security Staffing Requirement

E - monitor staffing requirements; and
A - direct security staffing.

(5) Background Investigations

A - monitor background investigations of personnel assigned.

(6) Termination Process

I - identify the requirement for termination of an employee's access to a system; and
A - comply with established policies and procedures when terminating the employee's access to an IS.

b. Policy & Procedures

(1) Emergency Destruction

A - develop policies and procedures for the destruction of hardware, software, and firmware under emergency conditions.

(2) Access Control Policy (ACP)

I - report non-compliance with ACP; and
A - develop access control policies.

(3) Organizational Placement of IS/Information Technology (IT) Security Functions

I - monitor and report IS/IT security functions and report on effectiveness.

(4) Disposition of Classified Information

I - dispose of classified hardware and software in accordance with written instructions; and
A - develop procedures for disposing of classified hardware, software and firmware.

c. Education, Training, & Awareness

(1) Security Awareness

I - use and present security awareness materials; and
A - develop security awareness materials for IS users.

(2) Security Training

I - present security training to IS users;
I - monitor security training of all IS user; and
A - develop security training materials.

(3) Security Education

I - present security education to IS users/managers;
I - monitor security education of all IS users; and
A - develop/design IS education programs.

d. General Information

(1) Organization Culture

I - monitor the organization's culture and it's affect on the security of an IS.

(2) Basic/Generic Management Issues

I - identify basic management issues and their impact on an IS security program.

e. Operations

(1) Account Administration

E - establish user accounts in accordance with policy;
I - develop security policy for account administration; and
A - conduct oversight for account administration.

(2) Intrusion Detection

E - test operability of physical intrusion detection systems.

(3) Backups

E - outline security policy for backup procedures;
I - review backup policy; and
A - enforce compliance with backup policy.

(4) Password Management

E - issue passwords;
I - enforce control and use of passwords in accordance with policy, procedures and requirements; and
A - develop password management policy.

5. Enforce security policies and safeguards on all personnel having access to the IS for which the ISSO is responsible

a. Oversight

E - list local and command security policies and safeguards;
I - enforce security policies and safeguards; and
A - develop local security policies and safeguards.

b. Management of the Security Function

(1) Customer Service Orientation

E - promote basic security policies and safeguards.

6. Ensure audit trails are reviewed periodically (e.g., weekly, daily), and audit records are archived for future reference, if required

a. Auditing Tools

(1) Audit Trail and Logging

E - follow audit policy and procedures;
E - activate required audit features;
E - review audit trail/log, as required;
I - monitor the use of audit trails and logging;
I - analyze audit trail/log for anomalies;
I - report audit anomalies;
A - develop policy and procedures on the use of audit trails and logging; and
A - define required audit features.

(2) Error Logs/System Logs

E - follow policy and procedures;
E - review error logs/system logs, as required;
I - monitor the use of error logs/system logs;
I - analyze error logs/system logs for anomalies;
I - report anomalies; and
A - develop policy and procedures on the use of error logs/system logs.

(3) Monitoring

(a) Electronic Monitoring (EM)

E - outline known means of electronic monitoring; and
I - use results of EM reports.

(b) Keystroke Monitoring

E - outline keystroke monitoring policy and procedures;
E - comply with keystroke monitoring policy and procedures;
I - enforce the use of keystroke monitoring in compliance with policy; and
A - develop keystroke monitoring policy and procedures in compliance with legal requirements.

(4) Protective Technology

(Note: not applicable to entry or intermediate level and must be monitored for events by the advanced level when applicable.)

A - integrate the use of protective technology; and

A - monitor the use of protective technology.

(5) Automated Security Tools

E - list and be able to identify by name various tools;
I - integrate the use of automated security tools; and
I - monitor the use of automated security tools.
E - use expert system tools (i.e., audit reduction and intrusion detection) available;
I - analyze results from expert systems and make recommendations for improvement; and
A - evaluate products and recommend acquisition of expert systems tools to management.

b. Configuration Management

I - integrate IS security requirements into the configuration management program;
I - review proposed changes to the configuration and recommend change based on security requirements;
I - perform security testing prior to implementation ensuring changes made to the systems do not violate security policy; and
I - require accountability of copyrighted software in accordance with software licensing agreements.

c. Audit

(1) Reconciliation

E - monitor the reconciliation of audit logs.

(2) Security Reviews

E - monitor the use of security reviews; and
I - prepare security reviews.

(3) Metrics

E - monitor the use of metrics.

(4) Conformance Testing

E - monitor conformance testing.

(5) Contingency Plan Testing

E - develop contingency plan testing procedures; and
E - monitor contingency plan testing.

(6) Disaster Recovery Plan Testing

E - develop disaster recovery plan testing; and
E - monitor disaster recovery plan testing.

(7) Alarms, Signals, & Reports

E - monitor the use of alarms, signals, and reports.

(8) Periodic Review of Audit Trails

I - direct the use of periodic reviews of audit trails.

d. Policies

(1) Change Control Policies

E - develop change control policies;
E - monitor change control policies;
E - revise change control policies; and
E - upgrade change control policies.

(2) Agency Specific Security Policies

E - monitor agency specific security policies; and
E - develop agency specific security policies.

7. Initiate protective or corrective measures

a. Intrusion Deterrents

E - list local and command security policies and safeguards;
I - enforce security policies and safeguards; and
A - develop local security policies and safeguards.

(1) Alarms, Signals, & Reports

I - choose balance between hardware, software, and/or procedural indicator schema; and
I - use analysis of intrusion indicators, when appropriate, and generate reports.

(2) Intrusion Detection

E - define intrusion detection system;
I - use appropriate intrusion detection system; and
I - select appropriate intrusion detection deterrents.

b. Network Security

E - describe national level policy for a specific network;
E - explain the need for security on the system and interconnected networks; and
A - explore vulnerabilities of leading edge emerging technologies.

(1) Lines (Fiber, Copper, Wireless)

E - describe the types of lines used in networks; and
E - explain appropriate security measure for each type of line.

(a) Leased

E - describe the security implications of leased lines; and
E - identify the security needs for leased lines.

(b) Owned

E - describe the security implications of owned lines; and
E - identify the security needs for owned lines.

(2) Off-site Security

I - assist in determining the off-site security requirements as they impact on the local system or network (need to ensure the other unit does not degrade yours);
E - describe the meaning of off-site security;
I - provide inputs to the design of any features needed to maintain security at an off-site location;
I - determine the off-site security requirements as they impact on the local system or network (need to ensure the other unit does not degrade yours); and
I - write status reports on off-site security to management.

(3) FAX Security

E - describe what is entailed by FAX security and its vulnerabilities;
E - explain difference between stand-alone FAX machines and FAX boards on computers; and
I - develop procedures governing FAX security.

(4) Network Firewalls

E - describe network firewall and its uses;
E - use/make sure the firewall is used; and
I - recommend appropriate firewall technology based upon network connections and vulnerabilities.

(5) Switch

E - describe a switch and its uses; and
I - ensure protection measures are used for switches.

(6) Phone Mail

E - describe phone mail and its uses; and
E - identify potential vulnerabilities on single lines used by many people.

(7) Modems

E - describe function of a modem and its uses;
E - identify potential vulnerabilities with modems when shared among systems; and
I - develop policy and practices regarding modem security.

c. Marking of Media/Information Systems Oversight Office (ISOO) Rules

E - describe the ISOO rules as published in the Federal registry and its implementation in the system; and
I - develop local implementing policy.

(1) Labeling

E - describe the marking and release rules to users and managers.

(2) Marking of Sensitive Information

E - describe the policy to mark all sensitive information and how to do it.

d. Environmental Controls

E - identify controls that are needed;
E - describe what is meant by environmental controls; list potential benefits and hazards of some;
E - provide examples of controls; and
I - assure controls are used and maintained.

(1) Fire Prevention

E - describe the requirement and identify measures in place.

(2) Safety

E - describe the requirement and identify measures in place.

(3) Filtered Power

E - describe the requirements and identify measures in place.

(4) Grounding

E - describe what is meant, the requirement, and identify measures in place.

e. Assessments (e.g., surveys, inspections)

E - assist customers on how to best use resources;
I - perform surveys or inspections;
I - report findings and recommendations; and
A - prioritize findings and recommendations.

(1) Validation Testing

I - report findings and recommendations;
A - defend findings among the participating components; and
E - define what is meant and encompassed by validation testing.

(2) Traffic Analysis

E - define traffic analysis;
I - summarize the information inferred from observations and provide reports; and
I - use the information to our advantage and the other party's detriment.

(3) Evidence Collection

I - answer questions from management about potential vulnerabilities;
I - assist in making recommendations on the findings based on evidence collection;
E - describe what is meant by evidence collection and its importance to assessment and management;
I - provide examples relating to various criminal situations in IS; and
I - identify potential problems.

f. Handling Media

E - list national and command policies, procedures, and rules regarding media handling;
E - assist users and managers in complying with rules, regulations, etc.; and
I - relate current policy to new situations.

(1) Remanence

E - describe the phenomenon and its implication to various types of media; and
E - describe the command/agency remanence program to users and managers.

(2) Physical Controls & Accounting

E - list policies and procedures; and
E - describe the policies and procedures to users.

(3) Transportation

E - list policies and procedures; and
E - describe the policies and procedures to users.

8. Report security incidents in accordance with agency-specific policy to the DAA when an IS is compromised

a. Security Violations Reporting Process (incident response)

E - describe the process of responding and reporting of security incidents;
E - comply with agency specific/local directives when reporting to the DAA;
I - assist users and managers with incident response;

I - organize an incident response team;
I - report results of an incident response;
A - evaluate damage done by an incident; and
A - propose actions, changes, modifications to the INFOSEC program and practices based upon an incident.

b. Security Investigation Procedures

E - describe the process of investigating security procedures;
E - follow the procedures;
E - identify the investigating authorities;
E - assist in investigations as requested;
I - monitor compliance with procedure;
I - explain the procedures to users and managers, the significance of the actions, and the consequences for variations;
I - propose changes to procedures; and
A - design the investigation procedures with appropriate authorities.

c. Law

(1) Investigative Authorities

E - identify the agencies and offices responsible for investigating security incidents; and
I - explain to users and managers the roles of various authorities.

(2) Law Enforcement Interfaces (LEI)

E - describe how the ISSO interfaces with law enforcement agencies;
E - describe how to contact and use assistance from LEI; and
A - improve effective coordination with LEI.

(3) Witness Interviewing/Interrogation

E - describe the proper procedures to follow when conducting a witness interview;
E - identify who can conduct interrogations (investigative agencies only); and
E - assist appropriate authority in witness interviewing/interrogation.

(4) Entrapment

E - define entrapment;
I - monitor entrapment techniques which are instituted for compliance with policies and guidelines; and
A - design entrapment stratagems in coordination with appropriate authorities.

(5) Disgruntled Employees

E - identify the proper procedures for handling disgruntled employees;
E - monitor handling of disgruntled employees in accordance with established procedures; and

I - design the procedures to handle disgruntled employees in coordination with appropriate authorities.

(6) Civil/Criminal Penalties

E - describe the possible civil/criminal penalties resulting from security incidents.

9. Report the security status of an IS, as required by the DAA

a. Administrative Security Policies and Procedures

E - explain the necessity of following administrative security policies and practices;
E - comply with administrative policies and procedures;
I - monitor compliance with administrative security policies and procedures;
I - prepare report of non-compliance to the DAA;
I - propose modifications to current policies and procedures;
A - recommend corrective/remedial action for non-compliance;
A - devise policies and procedures; and
A - revise current policy and procedures.

b. Agency Specific Security Policies

E - describe how agency specific policies enhance the overall security posture of an IS by defining the operational environment;
I - comply with agency specific security policies when reporting the security status to the DAA.

(Note: see paragraph 9a; the functions are the same in this area.)

c. Computer Emergency Response Team (CERT), Automated Systems Security Incident Support Team (ASSIST), Trade Journals, Bulletin Board System (BBS) Notices

E - explain how other sources of information can assist the ISSO in determining the security status of an IS;
I - compile information from various sources for application to local program;
A - develop information dissemination plan; and
A - interpret IS security information for implications on local systems.

10. Evaluate known vulnerabilities to ascertain if additional safeguards are needed (risk management)

a. Threats

E - define threats.

(1) Human Threats

E - describe how people can threaten a system’s security;
E - describe types of human threats to a system (insider, outsider, hacker, unauthorized user);
I - identify suspicious activity on a system;
A - proposes/develop countermeasures to identified threats;
E - describe how industrial espionage can impact the security of an IS; and

E - describe how international espionage can impact the security of an IS.

(2) Environmental/Natural Threats

E - describe the threat from electronic emanations;
E - identify appropriate TEMPEST authorities;
E - describe the threat from floods;
I - identify flood countermeasures;
E - describe the threat from fire;
I - identify fire-related countermeasures;
E - describe the threat from earthquake;
I - identify earthquake-related countermeasures;
E - describe the types of environmental controls (air conditioning, filtered power, etc.); and
I - monitor the impact of environmental controls on systems operations.

(3) Technological Threats (Commercial Off-The-Shelf (COTS), Development, Maintenance)

E - define technological threats;
I - identify the sources of technological threats: hardware, software (operating systems, applications, malicious code), firmware, networks (local area networks, wide area networks, metropolitan area networks, and direct connect);
I - describe countermeasures to known threats/vulnerabilities; and
I - propose new countermeasures to threats/vulnerabilities.

(4) Security Reviews

E - describe how security reviews can be used to identify threats to an IS.

b. Vulnerability Analysis

E - describe vulnerability analysis;
E - assist in the performance of vulnerability analysis;
I - conduct/perform vulnerability analysis;
A - analyze the results of a vulnerability analysis;
A - recommend fixes for deficiencies identified by the vulnerability analysis; and
A - recommend approval/rejection to the DAA of a system based on vulnerability analysis.

c. Countermeasures

E - describe how countermeasures can reduce the impact of threats.

(1) Evaluated Products

E - define evaluated products/Evaluated Products List (EPL);
E - know how to use evaluated products;
I - integrate evaluated products into a system; and
A - recommend evaluated products for use in a system.

(2) Technical Surveillance Countermeasures

E - describe technical surveillance countermeasures;
I - monitor technical surveillance;
A - recommend starting/stopping surveillance to the DAA; and
A - develop procedures for performing surveillance.

(3) Disaster Recovery

E - define disaster recovery;
E - describe the need for disaster recovery;
I - review disaster recovery plans; and
I - review results of annual tests of recovery plans.

(4) Third Party Evaluation

E - describe how third party evaluations can be used as a countermeasure;
I - interpret results of third party evaluations; and
A - recommend acceptance or rejection of system based on third party evaluation to the DAA.

(5) Security Reviews

E - discuss how security reviews can be used as a countermeasure;
I - conduct annual security reviews;
I - develop plans for annual security reviews;
A - interpret results of annual security reviews;
A - recommend changes to appropriate authorities; and
A - develop policies for conducting security reviews.

(6) Cost/Benefit Analysis

E - define cost/benefit analysis;
I - conduct cost/benefit analysis procedures; and
A - recommend changes to the DAA based on results of a cost/benefit analysis.

(7) Security Policies & Procedures

E - describe how effective security policies and procedures can reduce threats to an IS;
E - identify security policy-making bodies;
I - write local guidance; and
A - interpret policy and procedures.

d. Risks

E - define risk and residual risk (threat and vulnerability pairs).

(1) Risk Assessment

E - define risk assessment; and
I - describe the risk assessment process to include:

(a) risk assessment

E - define information criticality; and
I - estimate information criticality.

(b) information states

E - describe the three states of information.

(c) information valuation

E - define information valuation; and
I - estimate information valuation.
I - conduct risk assessments;
I - write risk assessment reports;
A - develop policy and procedures for conducting a risk assessment;
A - coordinate resources to perform a risk assessment; and
A - interpret results of a risk assessment.

(2) Risk Acceptance

E - define risk acceptance;
I - describe the risk acceptance process;
A - recommend actions to management based on risk acceptance; andA- recommend accreditation of a system to the DAA based on risk assessment.

ANNEX B

REFERENCES

The following references pertain to this Instruction:

a. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November 1992

b. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, dated June 5, 1992

c. DoD 5200.28-M, Automated Data Processing Sucurity Manual, dated January 1973

d. NCSC-TG-027, Version 1, AuGuide To Understanding Information System Security Officer Responsibilities for Automated Information Systems, dateed May 1992

e. DCID 1-16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, dated July 19, 1988

ANNEX C

BIBLIOGRAPHY

1. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988

2. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990

3. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996

4. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act, dated January 3, 1992

5. National Computer Security Center TG-005, Trusted Network Interpretation (TNI), dated July 31, 1987

6. DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985